UVIC KNOWLEDGE

Research and discovery
at the University of Victoria

VOL 16 NO 9 NOV 2016

CYBER SAFE

Traoré. UVIC PHOTO SERVICES

UVic cyber-security researchers aim to stay one step ahead of computer hackers

by Patty Pitts

Your kitchen microwave oven may look benign. But if it's in a "smart home" where appliances are part of an integrated system operated remotely through computer devices like smartphones, your oven could be the portal through which hackers gain access to your entire computer system.

As digital technology becomes increasingly integrated and more advanced, so too does the threat to cybersecurity. The University of Victoria's Information Security and Object Technology research lab has been addressing this threat since 1999. Coordinator and research engineer Issa Traoré admits it's a constant battle to keep ahead of hacker expertise and adaptability.

"There's no such thing as a 100 per cent secure system," says Traoré, citing the case of a premier cybersecurity company that was hacked. "Challenging and questioning systems is a very important part of security research. You have to be a skeptic. You have to look for flaws."

In the lab's early days, password protection was paramount. Then the next level of security became biometrics, requiring users to submit iris or fingerprint scans. But fingerprint scanners were "bulky and cumbersome," remembers Traoré. He started looking for other ways to identify users.

The lab focused on "behavioural biometrics," which develops user profiles based on the individual patterns of keyboard, mouse and swipe pad use.

The result was BioTracker, a security system that continuously authenticates a user by monitoring mouse and keystroke behaviour throughout a computer session. Any deviation from those usual use patterns, and the session ends.

Traoré developed BioTracker with his former PhD student Ahmed Awad and the technology became the backbone of Plurilock Security Solutions, a company created in 2008 through the support of UVic Industry Partnerships. Traoré is the company's chief scientist.

Plurilock clients, mainly in the US, install BioTracker on their existing systems. "Our strategy is to work with system integrators—companies that already have their own security software—to use BioTracker as an additional layer of protection," says Traoré.

Yet even as he leads the lab team of graduate students to develop more sophisticated cybersecurity software, Traoré is aware of the difficulty in keeping one step ahead of those working just as hard to breach those systems.

His team is currently working on better security to tackle "botnets"—networks of hacked computers—that can seize control of a computer through the conventional method of spam email containing lethal links. The botnet, operated domestically or in another country, uses that machine to establish a connection with a hacked server.

"The human behind the botnet, the 'bot master,' can then give orders that affect all machines connected to the server," says Traoré. "Lots of machines can be infected without anyone knowing."

As for that lurking microwave, when connected to other "smart" equipment such as security systems, webcams and hand-held computers, it becomes part of an internet of things, or IOT.

"Developing better IOT security is another priority for us," says Traoré, who says that awareness about cybersecurity remains low—even among sophisticated systems users.

"People wait for a problem and then look for a solution instead of being proactive. Our team is always questioning how to make better systems so we can get in front of the hackers."

EDGEWISE

Public Safety Canada defines cyberspace as "a global commons where more than 1.7 billion people are linked together." The agency adds that 1.7 million Canadians were victims of identity theft in 2008 (last figures available), estimating an annual cost to the country of nearly $1.9 billion.

Worried about your computer security at home? Avoid using familiar passwords such as names, telephone numbers or birthdays. Instead use at least eight characters with a mix of capital letters, symbols and numbers. And never click on file attachments or weblinks contained in emails from strangers.

Biometrics is now entrenched in our everyday lives. Airports use iris scanners for security, cars use voice recognition to activate Bluetooth or other entertainment systems, and many smartphone users unlock their phones through fingerprint scans. Passport Canada has used facial recognition technology since 2009.

Popular courses taught by Traoré and his grad students include ethical hacking and network protection techniques, and ways to collect and analyze digital evidence related to cybercrimes and other criminal activities involving electronic devices.

Housed in UVic's Faculty of Engineering, the Information Security and Object Technology lab has graduated four postdoctoral fellows, 11 PhD and 18 master's students since its inception. Some are teaching at institutions around the world while others are working in the cybersecurity industry.